

1 April 2009

By: Lucian Constantin, Web News Editor

## [Google: Spam Volume Back to pre-McColo Takedown Levels](#)

*Cybercrooks are building a more robust spam-distribution infrastructure*



Spam distribution fully recovered after the McColo takedown  
Umut Pulat

Google has [released](#) its "Spam data and trends" report for the first quarter of 2009. According to the statistics compiled by the Google security and archiving team, during the last half of March, the weekly spam volume has been the same as before the McColo ISP, a former cybercrime haven shut down last November.

The Mountain View search giant estimates that its e-mail security solutions have been used by over 50,000 businesses and 15 million business users around the world, amounting to a whopping three billion daily enterprise email connections. This allows the company to get an in-depth insight into the global spam trends.

One of the major wins for the IT security community in 2008 was the [takedown](#) of a U.S.-based hosting provider called McColo, following the combined efforts of several volunteer cybercrime-fighting groups, reporters and ISPs. Amongst other things, McColo was hosting the command and control servers for some of the largest spam-sending [botnets](#) on the Internet at the time. Its de-peering severely crippled the spam distribution infrastructure and resulted in a severe drop in the overall volume of junk e-mails.

"Spammers have clearly rallied following the McColo takedown, and overall spam volume growth during Q1 2009 was the strongest it's been since early 2008, increasing an average of 1.2% per day. To put that number into context, the growth rate of spam volume in Q1 2008 was approximately 1% per day - which, at the time, was a record high," Amanda Kleha of Google's security and archiving team announces.

This is consistent with the trend observed earlier this year by MessageLabs, a subsidiary of Symantec. At the end of January, the company specializing in electronic communication security [announced](#) that the spam activity had reached between 80%-90% of what it was before the McColo operation was shut down.

According to Ms. Kleha, junk e-mail levels are not just back-up, but they are here to stay, as the spammers have taken precautions against suffering similar crippling blows in the future. "[...] Data suggests they're adopting new strategies to avoid a McColo-type takedown from occurring again. Specifically, the recent upward trajectory of spam could indicate that spammers are building botnets that are more robust but send less volume - or at least that they haven't enabled their botnets to run at full capacity because they're wary of exposing a new ISP as a target," she explains.

Another noteworthy development resulting from Google's data is an increase in [localized spam](#). This involves customizing the messages based on the location of the IP address of each victim, to make them more personal and relevant to their targets. Additionally, the number of e-mails with [malware attached](#) to them is also on the rise, being 9 times higher in March than in February.